

NOT MEASUREMENT
SENSITIVE

MIL-STD-2045-48501
25 JANUARY 1995

MILITARY STANDARD

COMMON SECURITY LABEL (CSL)



AMSC N/A

AREA DCPS

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

FOREWORD

This military standard is approved for use by all Departments and Agencies of the Department of Defense.

Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this MIL-STD should be addressed to:

Joint Interoperability and Engineering Agency(JIEO)
ATTN: TBBD
Building 286
Fort Monmouth, New Jersey 07703-5613

by using the Standardization Document Improvement Proposal (DD form 1428) appearing at the end of this MIL-STD or by memorandum.

The preparing Agency for this standard is the Data Communication Protocol Standards(DCPS) Technical Management Panel (DTMP). The custodians for the document are defined in the Defense Standardization Program, "Standard Directory(SD-1) and are classified in the Federal Supply Classification(FSC) system under Data Communication Protocol Standards(DCPS). Additional information can be obtained from:

Joint Interoperability and Engineering Agency(JIEO)
ATTN: TBBD
Building 286
Fort Monmouth, New Jersey 07703-5613

The CSL and the Standard Security Label (SSL) (FIPS 188) developed by NIST have been extensively coordinated so that the standards portion of both be essentially identical. In addition the CSL will be revised to reference the SSL once the SSL is published, however, the revised CSL will have no impact on Project Managers that implement this version of the CSL. The CSL differs from the SSL in that the CSL contains standards implementation guidance for DoD Program Managers with imminent acquisitions. No implementation guidance is contained in (or planned for) the SSL.

MILITARY STANDARD: COMMON SECURITY LABEL

Table of Contents

1. SCOPE.....	1
1.1 Scope.....	1
1.2 Content.....	1
1.3 Application.....	1
1.4 Objectives.....	1
2. APPLICABLE DOCUMENTS.....	2
2.1 Government Documents.....	2
2.1.1 Standards.....	2
2.2 Non-Government Publications.....	3
2.3 Order of precedence.....	3
3. DEFINITIONS.....	4
3.1 Definition of terms.....	4
3.1.1 Bit order.....	4
3.1.2 Destination system.....	4
3.1.3 DAC.....	4
3.1.4 DOI.....	4
3.1.5 DOI authority.....	4
3.1.6 DOI Identifier.....	4
3.1.7 End system.....	4
3.1.8 Intermediate System.....	5
3.1.9 ICMP.....	5
3.1.10 IP.....	5

3.1.11 ISO.....	5
3.1.12 Label range.....	5
3.1.13 MAC.....	5
3.1.14 MLS.....	5
3.1.15 Network byte order.....	5
3.1.16 Object.....	5
3.1.17 Protocol Data Unit.....	5
3.1.18 Release marking.....	5
3.1.19 Release category.....	6
3.1.20 Security attributes.....	6
3.1.21 Security domain.....	6
3.1.22 Sensitivity category.....	6
3.1.23 Sensitivity level.....	6
3.1.24 Source system.....	6
3.1.25 Subject.....	6
3.1.26 Vector, binary valued.....	6
3.1.27 Vector sum.....	6
3.1.28 Vector Product.....	6
4. GENERAL DESCRIPTION.....	7
5. DETAILED REQUIREMENTS.....	8
5.1 General.....	8
5.2 Header.....	8
5.2.1 Format.....	8
5.2.1.1 Security Label Identifier.....	8

5.2.1.2 Length of CSL.....	8
5.2.1.3 Domain of Interpretation (DOI) Identifier.....	9
5.3 General Tag Format.....	9
5.3.1 Format.....	9
5.3.2 Tag Type.....	9
5.4 Tags.....	10
5.4.1 Tag Type 1.....	10
5.4.1.1 Tag Type.....	10
5.4.1.2 Tag Length.....	10
5.4.1.3 Alignment Octet.....	10
5.4.1.4 Sensitivity Level.....	10
5.4.1.5 Bit Map of Categories.....	10
5.4.2 Tag Type 2.....	11
5.4.2.1 Tag Type.....	12
5.4.2.2 Tag Length.....	12
5.4.2.3 Alignment Octet.....	12
5.4.2.4 Sensitivity Level.....	12
5.4.2.5 Enumerated Categories.....	12
5.4.3 Tag Type 5.....	13
5.4.3.1 Tag Type.....	13
5.4.3.2 Tag Length.....	13
5.4.3.3 Alignment Octet.....	13
5.4.3.4 Sensitivity Level.....	13
5.4.3.5 Category Ranges.....	13

5.4.4	Tag Type 6	14
5.4.4.1	Tag Type	14
5.4.4.2	Tag Length	14
5.4.4.3	Alignment Octet	14
5.4.4.4	Sensitivity Level	14
5.4.4.5	Bit Map of Release Categories	15
5.4.5	Security Label Specifications	15
5.5	Tag Classes	17
5.5.1	Security Policy and Procedures	17
5.5.2	Registration of Unique Tag Types	17
5.6	Processing Procedures	18
5.6.1	Source System	18
5.6.2	Intermediate System	18
5.6.3	Destination System	19
5.6.4	Unlabeled PDUs	20
5.6.5	Unrecognized Tag Types	20
5.6.6	Error Processing	21
5.7.	MAC Sensitivity Security Class Tags	22
5.7.1	Policy	22
5.7.2	Processing Procedures	23
5.7.2.1	Source System	23
5.7.2.2	Intermediate System	24
5.7.2.3	Destination System	24
5.7.2.4	Specific Tag Procedures	24

	MIL-STD-2045-48501	
5.8	Release Markings Security Class Tags.....	25
5.8.1	Policy.....	25
5.8.2	Source System.....	26
5.8.3	Intermediate System.....	26
5.8.4	Destination System.....	26
5.8.5	Processing Tag Type 6.....	27
6.0	Key Words	28

1. SCOPE

1.1 Scope. This document establishes the specifications for the COMMON SECURITY LABEL (CSL). This protocol data unit enables the labeling of information as it passes through communications systems. The format of the CSL option makes it possible to include the CSL in the options section of communications protocols (such as the TCP/IP protocols or Transport Protocol Class 4 (TP4)/Connectionless Network Protocol (CLNP)) and for end and intermediate devices to parse the option and utilize the security information in the label.

1.2 Content. This document specifies the requirements to be met by complying systems. It is not the intent of this document to specify any particular hardware or software design for implementation.

1.3 Application. This standard is applicable to the Department of Defense and may be adopted by the Intelligence Community. The standard is applicable to the design and development of new equipment, assemblages, and systems. It is also applicable to the operation of existing systems but it is not intended that existing systems be immediately converted to comply with this standard. New equipment and systems, those undergoing major modification, or those capable of rehabilitation shall conform to this standard.

1.4 Objectives. The objectives of this document are: to provide system requirements that ensure interoperation of equipment and systems consistent with military requirements and to achieve the necessary degree of performance and interoperation in the most economical way. The standard provides a means to label data as it passes through communications systems; provides a labeling format which can be used by encryption and guard protocols can use in their decision making; and a format for communications which enables end systems then use to maintain security labels on stored and displayed data. This document does not specify security label formats for operating systems, DBMSs, etc. but is for communications systems usage.

2.1.1 Standards. The following standards form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the Department of Defense Index of Specifications and Standards (DODISS) and supplement thereto.

FED-STD-1037B - Telecommunications: Glossary
 of Telecommunications Terms,
 3 June, 1993

FIPS PUB 146-1 Government Open Systems
Interconnection Profile
(GOSIP), 3 April, 1991

NSTISSI No. 4009 National Information Systems
Security (INFOSEC) Glossary,
5 June 1992.

MIL-STD-2045-14502 DoD Standardized Profiles -
Internet Transport Profiles -
Part 1: Transport Services,
February 1994.

2

(800) 365-3NIC or (703) 802-8400, or as part of the DDN Handbook v.1., A166324, from the Defense Technical Center, Cameron Station, Alexandria, VA 22304-6145, telephone (703) 274-7633.)

2.2 Non-Government Publications. The following documents form a part of this document to the extent specified herein.

INTERNATIONAL STANDARDS

ISO 7498 - Open Systems Interconnection
 Basic Reference Model,
 International Organization
 for Standardization,
 Switzerland

(Copies of the above document are available from Omnicom, Inc., 115 Park Street, SE, Vienna, VA 22180-4607, telephone (800) 666-42660 or (703) 281-1135.)

RELATED STANDARDS

RFC 791 - Internet Protocol, Postel, J.B.1981

RFC 792 - Internet Control Message Protocol,
 Postel, J.B. 1981.

RFC 950 - Internet subnetting procedure
 Mogul, J.C. 1985

RFC 1108 - Security Options for the Internet
 Protocol, Kent, S. 1991.

(Information on how to obtain copies of the above is available from the Internet Network Information center (INTERNIC) telephone 800-444-4345.)

2.3 Order of precedence. In the event of a conflict between the text of this standard and the references cited herein, the text of this standard shall take precedence. Nothing in this standard, however, shall supersede applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Definition of terms. Definition of terms used in this document shall be as specified in FED-STD-1037. Those definitions of terms unique to this standard and not defined in FED-STD-1037 are provided in the following subparagraphs.

3.1.1 Bit Order: This is a standard ordering of bits as they are transmitted over a DDN or OSI network. Bits within bytes are transmitted from most significant bit (MSB) to least significant bit (LSB).

3.1.2 Destination system: This is the information system that is identified by the destination address in the protocol data unit header. This system will be the one to receive the protocol data unit and pass it to an upper layer protocol.

3.1.3 DAC: Discretionary Access Control is used to control access to objects based on the identity of subjects and/or the groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject at the subject's discretion.

3.1.4 DOI: A collection of systems that share a same set of security policies and a common interpretation of security attributes form a Domain of Interpretation (DOI).

3.1.5 DOI authority: The DOI authority is the organization that has obtained a DOI identifier. The authority is responsible for defining and requesting registration for and distributing the DOI mapping.

3.1.6 DOI Identifier: The DOI Identifier is the number used in the CSL header to uniquely represent a DOI.

3.1.7 End system: This refers to either the source or

destination system.

3.1.8 Intermediate System: A system performing functions of the lower three layers of the OSI Reference Model, commonly thought of as routing data for end systems.

3.1.9 ICMP: The Internet Message Control Protocol is a companion protocol to IP which provides feedback concerning problems in the communications environment.

3.1.10 IP: The Internet Protocol is a protocol above the network layer. It provides a connectionless service for end systems to communicate across one or more networks.

3.1.11 ISO: The International Organization for Standardization is an international agency which is a voluntary, nontreaty organization whose members are participating nations and nonvoting observer organizations.

3.1.12 Label range: This is a pair of security labels which detail the security labels a subject may access. It is assumed that all objects whose labels fall within this range, inclusive, are accessible by the subject.

3.1.13 MAC: Mandatory Access Control is a mechanism used to control access to resources based on the level of sensitivity as indicated by the security label. With MAC, the system controls access.

3.1.14 MLS: Multi-Level Security (MLS) is the practice of giving host or network resources a sensitivity label and restricting access to those resources based on a users clearance label range.

3.1.15 Network byte order: This MIL-STD assumes the most significant byte/octet is transmitted first.

3.1.16 Object: An object is a network resource to which access by a subject must be controlled in accordance with the local security policy. Examples of objects for networks are: protocol data units, applications, configuration parameters, connections, and networks.

3.1.17 Protocol Data Unit: A unit of data specified in a protocol and consisting of protocol information and, possibly, user data.

3.1.18 Release marking: A release marking provides a list

of authorized subjects who may access the associated object.
The release marking is made up of release categories.

3.1.19 Release category: The release category represents a subject or group of subjects that may access an object.

3.1.20 Security attribute: A security-related quality of an object.

3.1.21 Security domain: A collection of entities to which applies a single security policy executed by a single authority.

3.1.22 Sensitivity category: A sensitivity category is a security attribute that describes in absolute terms a protection requirement (i.e., is not related to a protection hierarchy.)

3.1.23 Sensitivity level: Security attribute that indicates a required level of confidentiality protection according to a predefined protection hierarchy. The level is hierarchical in ascending order, meaning that level N represents greater sensitivity than level N-1.

3.1.24 Source system: This is the information system that originated the protocol data unit with the CSL label.

3.1.25 Subject: The subject is an active entity that requests access to a particular object. Examples of subjects are hosts, network, computer processes, and users.
A subject can also be an object.

3.1.26 Vector, binary valued: An n-component binary-valued vector $A = (a_0, a_1, \dots, a_n)$ is an ordered list of n binary values $a_i = 0$ or 1.

3.1.27 Vector sum: The sum of two n-component binary-valued vectors $A = (a_0, a_1, \dots, a_n)$ and $B = (b_0, b_1, \dots, b_n)$ is $A + B = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n)$ where $0 + 0 = 0$ and $0 + 1 = 1 + 0 = 1 + 1 = 1$.

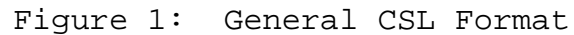
3.1.28 Vector Product: The product of two n-component binary-valued vectors $A = (a_0, a_1, \dots, a_n)$, and $B = (b_0, b_1, \dots, b_n)$ is $A \bullet B = (a_1 \bullet b_1, a_2 \bullet b_2, \dots, a_n \bullet b_n)$ where $0 \bullet 0 = 0 \bullet 1 = 1 \bullet 0 = 0$ and $1 \bullet 1 = 1$.

4. GENERAL DESCRIPTION

The CSL allows the attachment of specific security attributes associated with the data in a protocol unit. This data can be used to perform security decisions at communications layers. CSL can support a large set of security domains and policies with differing interpretations of security attributes. An extendible format allows for multiple sets of security attributes as well as the addition of new attribute types in the future.

This document defines the basic format and processing procedures for the CSL. In addition, it defines the specific attribute formats and procedures to support the DOD Mandatory Access Control Security Policy as well as a Release Markings Security Policy.

The basic format of the CSL is shown below. A fixed format header is followed by a variable length tag section.



5.2.1.3 Domain of Interpretation (DOI) Identifier

The DOI Identifier is 4 octets in length and stored in network byte order. The security attributes contained in the tag section will have meaning to systems within the same security domain as specified by the DOI.

DOI Identifier numbers supported must be configurable by the system administrator.

5.3 General Tag Format

Tags are independent data elements within a CSL that convey security attributes. A CSL will include 0 or more tags in any order. The purpose of tags is to provide an extensible method to pass security attributes using predefined formats and relating to a general security policy, such as DOD MAC security policy.

5.3.1 Format

The standard format for a CSL tag is shown below.

tttttttt	llllllll	iiiiiii . . .
----------	----------	---------------

Tag Type Tag Length Tag Information

Figure 3: General Tag Format

The tag type is one octet in length and is used to identify the specific format and processing procedures associated with the tag information field. The section below describes more on tag types. The tag length is one octet in length and gives the total octets in the tag including the tag type and length fields.

5.3.2 Tag Type

The tag type is a number between 0 and 255. Tag types 0 through 127 are used for standard tag definitions. For these standard tags the tag type number alone will identify the format for the tag information field. The DOI then determines the semantics for a given tag. This document defines standard tag types 1, 2, 5, and 6. Tag types 0, 3, and 4, and 7 through 127 are currently reserved for future use. Tag types 128 through 255 can be defined by the DOI

authority.

5.4 Tags

The three tags defined below represent three different ways to format a sensitivity label. Each of them store a sensitivity hierarchical level in a one octet field.

5.4.1 Tag Type 1

This is referred to as the "bit-mapped" tag type. The format of this tag type is as follows:

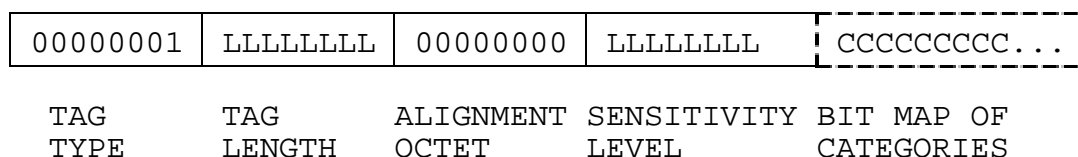


Figure 4. Tag Type 1 Format

5.4.1.1 Tag Type

This field is 1 octet in length and has a value of 1.

5.4.1.2 Tag Length

This field is 1 octet in length. It gives the total length of the tag in octets including the type and length fields.

5.4.1.3 Alignment Octet

This field is 1 octet in length and always has the value of 0.

5.4.1.4 Sensitivity Level

This field is 1 octet in length. Its value is a binary number with value from 0 to 255 decimal. The values are ordered with 0 being the minimum value and 255 representing the maximum value.

5.4.1.5 Bit Map of Categories

The length of this field is variable and ranges from 0 to 30 octets. This provides representation of sensitivity categories 0 to 239. The ordering of the bits is left to

right or MSB to LSB. For example category 0 is represented by the most significant bit of the first byte and category 15 is represented by the least significant bit of the second byte. Figure 5 graphically shows this ordering. Bit N is binary 1 if category N is part of the label for the protocol data unit, and bit N is binary 0 if category N is not part of the label. Minimal encoding should be used resulting in no trailing zero octets in the category bit map. That is, the final right octet in a bit map in a transmitted CSL should contain at least a single 1.

	octet 0	octet 1	octet 2	octet 3	octet 4
	XXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX
bit	01234567	89111111	11112222	22222233	33333333
number		012345	67890123	45678901	23456789

Figure 5. Ordering of Bits in Tag 1 Bit Map

A bit map is a binary-valued vector $V = (v_0, v_1, \dots, v_{8n-1})$ where $v_i = 0$ or 1 and where n is the number of octets in the vector. Each category to be represented in the vector for a specific DOI is assigned a position in the vector corresponding to an i in a specific v_i . If the value of v_i is a 1 the category is in the CSL, if the value is 0 it is not. For example, if v_2 is assigned the category "suspect vehicle" and v_3 the category "suspect aircraft" then if $v_2v_3 = 01$ the CSL bit map indicates the marking "suspect aircraft" (and not "suspect vehicle.") The final rightmost octet in a transmitted CSL category bit map should contain at least one $v_i = 1$.

5.4.2 Tag Type 2

This is referred to as the "enumerated" tag type. It can be used to describe large sets of sensitivity categories. The format of this tag type is as follows:

00000010	LLLLLLLL	00000000	LLLLLLLL	CCCCCCCCCCCCCCCC...
TAG TYPE	TAG LENGTH	ALIGNMENT OCTET	SENSITIVITY LEVEL	ENUMERATED CATEGORIES

Figure 6. Tag Type 2 Format

5.4.2.1 Tag Type

This field is one octet in length and has a value of 2.

5.4.2.2 Tag Length

This field is 1 octet in length. It gives the total length of the tag type including the type and length fields.

5.4.2.3 Alignment Octet

This field is 1 octet in length and always has the value of 0.

5.4.2.4 Sensitivity Level

This field is 1 octet in length. Its value is from 0 to 255. The values are ordered with 0 being the minimum value and 255 representing the maximum value.

5.4.2.5 Enumerated Categories

In this tag, a category is represented by a numerical value rather than by a position within a bit map. The length of the enumerated category field is 0 to 251 octets. The length of each category number is 2 octets. Valid values for categories are 0 to 65534 decimal. Category 65535 is not a valid category value.

Since each category to be represented by the CSLs for a specific DOI is assigned a 16 binary-bit value, a table can be made of the assigned values. For example, if the category "suspect vehicle" is assigned the value 0000010000010010 and the category "suspect aircraft" the value 0000010000010011 a section of this table would be

```
0000010000010010 = suspect vehicle
0000010000010011 = suspect aircraft
```

Note that alphanumeric codes can be used to assign values to the 2 octet CSL enumerated category numbers. For example, if, for a specific DOI, SV is used for suspect vehicles and SA for suspect aircraft, the ANSI-ASCII codes for A, S, V are 10000011, 10100111, and 10101101 (with odd parity) and so the assignment would be

```
1010011110101101 = SV = suspect vehicle
```

10100111110000011 = SA = suspect aircraft

Each 2-octet number is a 16 binary-bit vector $V = (v_0, v_1, \dots, v_{15})$ where the $v_i = 0$ or 1. Each CSL tag type 2 then contains a list of vectors each representing a category. Each category associated with a CSL is then represented by a vector in the CSL list.

5.4.3 Tag Type 5

This is referred to as the "range" tag type. It is used to represent labels where all categories in a range, or set of ranges, are included in the sensitivity label. The format of this tag type is as follows:

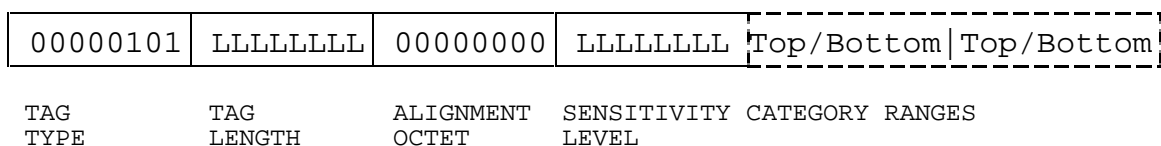


Figure 7. Tag Type 5 Format

5.4.3.1 Tag Type

This field is one octet in length and has a value of 5.

5.4.3.2 Tag Length

This field is one octet in length. It gives the total length of the tag type including the type and length fields.

5.4.3.3 Alignment Octet

This field is one octet in length and always has the value of 0.

5.4.3.4 Sensitivity Level

This field is one octet in length. Its value is from 0 to 255. The values are ordered with 0 being the minimum value and 255 representing the maximum value.

5.4.3.5 Category Ranges

A category range is a 4-octet field comprised of the 2-octet index of the highest-numbered category followed by the

2 octet index of the lowest-numbered category. These range endpoints are inclusive within the range of categories. All categories within a range are included in the sensitivity label. This tag may contain a maximum of 7 category pairs.

Figure 7 shows two categories pairs. The bottom category endpoint for the last pair in the tag may be omitted in which case it should be assumed to be 0. The ranges must be non-overlapping and be listed in descending order. Valid values for categories are 0 to 65534. Category 65535 is not a valid category value.

5.4.4 Tag Type 6

This is referred to as the "release markings" tag type. The format of this tag type is as follows:

00000110	LLLLLLLL	00000000	SSSSSSSS	CCCCCCCC.....
TAG TYPE	TAG LENGTH	ALIGNMENT OCTET	SENSITIVITY LEVEL	BIT MAP OF RELEASE CATEGORIES

Figure 8. Tag Type 6 Format

5.4.4.1 Tag Type

This field is one octet in length and has a value of 6.

5.4.4.2 Tag Length

This field is one octet in length. It gives the total length in octets of the tag type including the type and length fields.

5.4.4.3 Alignment Octet

This field is one octet in length and always has the value 0.

5.4.4.4 Sensitivity Level

This field is one octet in length. Its value is from 0 to 255. The values are ordered with 0 being the minimum value and 255 representing the maximum value.

5.4.4.5 Bit Map of Release Categories

The length of this field is from 0 to 251 octets. The bit map has one bit for each release category. All combinations are possible. The ordering of the bits is left-to-right or MSB to LSB. For example category 0 is represented by the most significant bit of the first byte and category 15 is represented by the least significant bit of the second byte. Figure 5 graphically shows this ordering. Bit N is binary 0 if release category N is part of the label for the protocol data unit, and bit N is binary 1 if release category N is not part of the label. Minimal encoding should be used resulting in no trailing all ones octets in the release category bit map.

The bit encoding used for release categories is the reverse of MAC category encoding where a binary 1 means that the category is included in the label. For release markings a 0 is used to indicate the category is included and a 1 that the category is not included. This inversion allows MAC category bit maps and release category bit maps to be treated the same when combining two objects together.

The release category bit map in a CSL is a vector $V = (v_0, v_1, \dots, v_{8n-1})$ where each v_i is a 0 or 1 and where n is the number of octets in the vector. Each category is associated with a bit position in the vector. If for a particular DOI, DIA is assigned v_3 and DEA v_4 , then $v_3 = 0$, $v_4 = 1$ would mean the protocol data unit's contents may be released to DIA and not to DEA. The vector transmitted would then be 11101111 if the protocol data was to be released only to DIA. (Notice the difference with a MAC type 1 tag. If a system has eight compartments A, B, ..., H and if a type 1 tag should represent B and D the bit pattern would be 01010000 in the bit map section.) The final octet in a transmitted CSL release category bit map should not be all 1s.

5.4.5 Security Label Specifications

The Abstract Syntax Notation 1 (ASN.1) definition of the Common Security Label (CSL) follows. This definition shall be encoded as appropriate to the layer where it will be used. The syntax is for the entire label including both tags and header.

ASN.1 Definition for the Common Security Label

```

CommonSecurityLabel      ::= SEQUENCE {
    domainName             DomainName
    securityTags           SEQUENCE OF SecurityTag
}

DomainName               ::= OBJECT IDENTIFIER

SecurityTag              ::= CHOICE {

    -- Bitmapped
    type-1                [1] IMPLICIT SEQUENCE {
        sensitivityLevel   SecurityAttribute,
        categoryFlags      BIT STRING
    }

    -- Enumerated
    type-2                [2] IMPLICIT SEQUENCE
        sensitivityLevel   SecurityAttribute,
        categoryList       SET OF
                            SecurityAttribute
    }

    -- Category ranges - pairs must be non-overlapping
    type-5                [5] IMPLICIT SEQUENCE {
        sensitivityLevel   SecurityAttribute,
        categoryRangeList  SET OF
                            SecurityAttributeRange
    }

    -- Release categories
    type-6                [6] BIT STRING
}

-- The upperBound must be greater than the lowerBound
-- The lowerBound of last pair can be empty (interpreted as
0)
SecurityAttributeRange   ::= SEQUENCE {
    upperBound            SecurityAttribute,
    lowerBound            Security Attribute }

SecurityAttribute        ::= INTEGER

```

5.5 Tag Classes

Tags are divided into tag classes. When used to support current DoD policy, the label numbers 1,2, and 5 defined in this document belong to the Mandatory Access Control (MAC) Sensitivity class and support the MAC Sensitivity Security policy. They each represent a different method for representing a MAC sensitivity label consisting of a level and a set of categories. Tag number 6 is a Release Category Tag.

5.5.1 Security Policy and Procedures

The security policy associated with a tag class defines how the attributes are to be used to make security decisions. A CSL may include multiple tags.

For current DoD systems and policy, the processing procedures below provide a detailed description of steps for transmitting packets from a "source" system, processing packets through an "intermediate" system, and receiving packets at a "destination" system. Section 5.6 describes the general processing procedures. Additional procedures specific to each tag class then follow.

In this document, source and destination systems are also known as "end" systems. Further, an intermediate system differs from an end system in that it does not process a protocol data unit above the (network) layer. End systems may also act as intermediate systems when forwarding packets between networks. Routers are examples of intermediate systems and need only implement the procedures defined for these systems.

5.5.2 Registration of Unique Tag Types

Contact DISA to request a unique DOI Identifier number. DOI defined tag types should be registered before use outside of a closed experimental network. To register a DOI tag type the DOI authority must submit the following information to DISA:

- a. Tag type number (> 127)
- b. Bit level format description of the tag
- c. Tag class name
- d. Description of the Security policy associated with the tag
- e. Detailed steps for processing the tag

5.6 Processing Procedures

The processing procedures defined in this section provide implementation guidance showing the basic procedures for TCP/IP that existing CSL implementations provide. Additional procedures then follow for specific tag classes.

5.6.1 Source System

The CSL source system performs the following steps prior to transmitting a protocol data unit. Some of these steps lead to auditable events for specific security policies.

- a. Get the required security attributes associated with the data to be included in the protocol data unit.
- b. Select a DOI to use based on the security attributes and destination address.
- c. End-system attribute values are converted to the values associated with the DOI chosen, if necessary.
- d. The appropriate tags are constructed to hold the security attributes and placed in the CSL.
- e. The CSL is placed in the header.
- f. The protocol data unit will be rejected if its transmission violates local security policy. A configuration parameter (which is a name for a programming variable) OUT-VIOLATION-MSG is used to determine if an error message is to be sent to the upper layer protocol. If OUT-VIOLATION-MSG is set to 1 then an error message is passed to the upper layer protocol. If OUT-VIOLATION-MSG is set to 0 then no message is sent. The default value for OUT-VIOLATION-MSG is 1. A log of all violations should be kept in an audit log.

5.6.2 Intermediate System

In the case that intermediate systems process the label, intermediate systems perform the following steps in processing each protocol data unit:

- a. Since an end system may also be an intermediate system, first determine whether the local system is the

destination for the protocol data unit. If it is, then the procedures described for destination system, Section 5.6.3, must be followed.

b. Locate the CSL in the header. If no CSL is found, then follow the instructions described in Section 5.6.4.

c. Ensure the DOI is supported by this system. If not then the protocol data unit is dropped and the instructions in Section 5.6.6 for "unrecognized label" are followed.

d. Process each tag within the CSL. If an unrecognized tag is found then follow the instructions in Section 5.6.5.

e. Using the security attributes and the associated security policies a check is made to determine if the PDU is allowed to enter the system. If the protocol data unit is refused then it is dropped and the instructions in Section 5.6.6 for "incoming violation" are followed.

f. If all checks pass then an algorithm will select the proper output to forward the PDU. (This algorithm may use the security attributes and the associated security policies to find a possible route.)

g. Using the security attributes and the associated security policies a check is made to determine if the PDU is allowed to exit the system. If a security violation is detected then the protocol data unit is dropped and the instructions in Section 5.6.6 for "forwarding violation" are followed.

5.6.3 Destination System

The following procedures will be followed when a system is the destination system for a protocol data unit. The policy for use of error correction codes in reconstructing received PDUs will be determined by the system security authority. Some of the following steps may lead to auditable events in specific security policies.

a. Locate the CSL. If no CSL is found then follow the instructions described in Section 5.6.4. If more than one CSL is included in the PDU then the protocol data unit is dropped and the instructions in Section 5.6.6 for "CSL missing" are followed.

b. Ensure the DOI is supported by this system. If not the protocol data unit is dropped and the instructions in Section 5.6.6 for "unrecognized label" are followed.

c. Process each tag within the CSL. If an unrecognized tag is found then follow the procedures described in Section 5.6.5.

d. Using the security attributes and the associated security policies a check is made to determine if the PDU is allowed to enter the system. If the protocol data unit is refused then it is dropped and the instructions in Section 5.6.6 for "incoming violation" are followed.

e. If required, the security attributes are converted to their local DOI representation.

f. The data in the packet and the security attributes are passed (made available) to the subject identified in the address section.

5.6.4 Unlabeled PDUs

Some current system inputs do not require a CSL label for all incoming protocol data units. When this configuration is used a default CSL will be associated with all incoming unlabeled protocol data units for this particular input channel. If this capability is not used the default condition is that a CSL is required for all incoming data units. If a CSL is required and one is not found in the data unit then the unit is dropped and the instructions in Section 5.6.6 for "CSL missing" are followed.

The configured default CSL may be inserted in the incoming protocol data unit. Insertion of the default CSL into the PDU may require additional modifications to the network header (e.g. new values for the header checksum or length). If a CSL cannot be inserted in the PDU because it is too large to fit in the header area then the PDU is dropped and the instructions in Section 5.6.6 for "incoming violation" are followed.

5.6.5 Unrecognized Tag Types

The default condition for any CSL implementation is that an unrecognized tag type must be treated as an error and the protocol data unit is dropped and the instructions for

an "unrecognized label" in Section 5.6.6 are followed.

5.6.6 Error Processing

This section refers only to IP systems and selected ISO systems at layer 3. It shows procedures which have been instituted for a number of existing systems and gives an example which can be used for developing error handling in other systems. In IP terminology an ICMP refers to an Internet Control Message Protocol which is used to handle error messages. In some situations, returning an ICMP message may violate security policy. The configuration parameter IN-VIOLATION-MSG is used to determine if an ICMP message may be returned. If IN-VIOLATION-MSG is set to 1 then ICMP messages may be returned. If IN-VIOLATION-MSG is set to 0 then no ICMP message may be sent in response to a CSL problem. Under no conditions will an ICMP message be returned when the problem occurs due to reception of an ICMP message. The default value for IN-VIOLATION-MSG is 0.

For layer three IP and selected ISO systems, the following table shows the specific message to return, if allowed by IN-VIOLATION-MSG, and any special handling restrictions.

Condition	Action
CSL missing	An ICMP "parameter problem" (type 12) is generated and must be returned to the originator through the same input channel from which it was received. The code field of the ICMP is set to "CSL missing" (code 1) and the ICMP pointer is set to 134.
unrecognized label	An "ICMP parameter problem" (type 12) is generated and must be returned to the originator through the same input channel from which it was received. The ICMP code field is set to "bad parameter" (code 0) and the pointer is set to the start of the CSL field that is unrecognized.

incoming violation	An ICMP "destination unreachable" (type 3) is generated and must be returned to the originator through the same input channel from which it was received. The code field of the ICMP is set to "communications with destination host administratively prohibited" (code 10).
forwarding violation	An ICMP "destination unreachable" (type 3) is generated and returned to the originator. The code field of the ICMP is set to "communication with destination network administratively prohibited" (code 9).

5.7. MAC Sensitivity Security Class Tags

5.7.1 Policy

The current MAC Sensitivity Security Policy (MSSP) is based on the standard model within the DOD for protecting sensitive paper documents. The following procedures provide implementation guidance for systems which want to implement this policy.

The MSSP is based on objects and subjects. The object is the contents of the protocol data unit. A subject is anything that may send or receive the protocol data unit such as a network input or output channel, host, or application. Each object is assigned a sensitivity label. The label is made up of a "sensitivity hierarchical level" (SHL) and a set of "sensitivity categories" (SC). A subject is assigned a range of labels which it is authorized to receive (RECEIVE-SL-RANGE) and another range which it is authorized to send (TRANSMIT-SL-RANGE). The range is composed of a "High Sensitivity Hierarchical Level" (HSHL), a "Low Sensitivity Hierarchical Level" (LSHL), and a set of "Authorized Sensitivity Categories" (ASC). The SHL, SC, HSHL, LSHL, and ASC are numbers which have a one-to-one mapping to a human readable sensitivity level or set of

sensitivity categories.

A particular action is allowed if the object's label falls within the subject's authorized range for that action.

For this to be true the following conditions must be true:

1. Object's SHL must be greater than or equal to the subject's LSHL.
2. Object's SHL must be less than or equal to the subject's HSHL.
3. All of the categories in the Object's SC must be included in the subject's ASC.

If the three conditions are not met then the objects label is not "within range", and the action is denied, refer to paragraph 5.6.6.

5.7.2 Processing Procedures

The following processing procedures are added to the procedures defined in Section 5.6. All label comparisons will be made with the appropriate DOI representation of the sensitivity label or range.

5.7.2.1 Source System

a. Determine tag type to use to carry the object's SHL and SC. If the category list cannot fit into one of the tags then the message is discarded. A message will be sent to the upper protocol if the OUT-VIOLATION-MSG is set to 1.

b. After the proper output channel is selected the protocol data unit's Sensitivity Label will be checked against the output channel's SL-RANGE-PORT-OUT Label range.

If the label is "within range" then the protocol data unit may be released through the output channel. If the protocol data unit's label is out of range then follow the instructions in Section 5.6.1, step f.

5.7.2.2 Intermediate System

a. Find the MAC Sensitivity Security Class tag in the CSL. If no tag of this class is found then drop the protocol data unit and follow the instructions specified in Section 5.6.6 for "unrecognized label".

b. Check to see if the protocol data unit's Sensitivity Label is "within range" of the SL-RANGE-PORT-IN

label range. If so then the protocol data unit may be accepted. If it is out of range then the protocol data unit is dropped and the instructions specified in Section 5.6.6 for "incoming violation" are followed.

c. After the proper output channel is selected the protocol data unit's Sensitivity Label will be checked against the TRANSMIT-SL-RANGE Label range. If the label is "within range" then the protocol data unit may be released.

If the protocol data unit's label is out of range then the protocol data unit is dropped and the instructions specified in Section 5.6.6 for "forwarding violation" are followed.

5.7.2.3 Destination System

Follow procedures a and b described in Section 5.7.2.2 above.

5.7.2.4 Specific Tag Procedures

The basic rule for processing tags is that every test associated with each tag in a CSL must be passed in order for the CSL to be forwarded. If a CSL contains a type 1 tag and a type 6 tag then the test for sensitivity hierarchical level must be passed followed by the type 1 tag bit map test followed by the release markings bit map test. Only if all tests are passed is the CSL forwarded.

The sensitivity hierarchical level test for a type 1, 2, or 5 tag consists of seeing if the binary number in the sensitivity level section is within the prescribed range. A CSL processing element has a stored eight bit lower range value of B_l and a stored upper range value of B_u , where B_l and B_u are binary numbers with decimal values 0 to 255 and $B_l \leq B_u$. Both B_l and B_u can be set by the system security managers. If the CSL sensitivity level section has the value B the CSL passes only if $B_l \leq B \leq B_u$.

If the CSL carries a type 1 tag the processor will store a vector V_s (which can be set by the system security manager) which has 1s in each position which corresponds to a category the subject can receive (or send if it is a transmitting test, or pass if it is an intermediate test.)

Every 1 in the CSL bit map must correspond to a 1 in V_s in order for the test to succeed and the CSL to be forwarded.

For the type 2 tag the CSL processor for a specific DOI will have a stored list of 2-octet binary values $L_s =$

$(V_1^s, V_2^s, \dots, V_m^s)$ where each $V_i^s = (v_0, v_1, \dots, v_{15})$; $v_j = 0, 1$, and each V_i^s corresponds to a category. Call the list of two octet enumerated values in a CSL type 2 tag $L^c = (V_1^c, V_2^c, \dots, V_m^c)$ where the V_k^c are 2-octet vectors. Then each 2-octet vector in L^c must also be in L_s in order for the test to be passed.

For the type 5 "range" tags the same list L_s used for type 2 tags in the processor for a specific DOI is used. Then if the TOP/Bottom pair T_p/B_p , where T_p and B_p are 2-octet vectors, occurs in a CSL type 5 tag, each binary value B_j must occur in L_s for $B_p \leq B_j \leq T_p$ in L_s . Here the values in L_s and T_p , B_p and B_j are all considered to be binary values from 0 to 255.

5.8 Release Markings Security Class Tags

5.8.1 Policy

The Release Markings Security Policy (RMSP) is equivalent to the MAC Sensitivity Security Policy except that its labels are made up of release categories. In addition, the processing of the release categories is different than the sensitivity categories. This section provides implementation guidance for processing in this area.

The object (i.e. the protocol data unit) will have a set of "Object Release Categories" (ORC) associated with it.

This is essentially a list of which subjects may receive the protocol data unit. A subject will have a set of "Subject Release Categories" (SRC) associated with receiving and sending protocol data units. The receiving list identifies on whose behalf the subject can act when receiving protocol data units. The sending list identifies on whose behalf the subject can act for sending protocol data units. If any release category in the ORC matches a release category in the SRC then the action is allowed.

For example, suppose we have a protocol data unit CSL with a release category list that includes just FBI and Coast Guard (CG). This protocol data unit is sent to host A and host B. Host A has an SRC list of DIA, DEA, and NSA. The protocol data unit would be rejected since the two lists do not share at least one category. Host B, however has an SRC list of CG, DEA, and DIA. It could receive the protocol data unit because both lists share the release category "CG". Notice that Host B's SRC list did not have to contain

the release category "FBI" to receive the protocol data unit.

An SRC list for incoming protocol data units RELEASE-CATEGORIES-PORT-IN will be configurable. An SRC list for outgoing protocol data units RELEASE-CATEGORIES-PORT-OUT will also be configurable.

5.8.2 Source System

After the proper output channel is selected the protocol data unit's ORC list will be checked against the RELEASE-CATEGORIES-PORT-OUT list. If the two lists share at least one category then the protocol data unit is released. If they share no categories then follow the instructions in Section 5.6.1, procedure f.

5.8.3 Intermediate System

The steps to be taken are:

a. Find the Release Sensitivity Security Class tag in the CSL. If more than one tag exists of this class then drop the protocol data unit and follow the instructions specified in Section 5.6.6 for "unrecognized label".

b. If the tag is present then compare its ORC list against the RELEASE-CATEGORIES-PORT-IN list. If the two lists share at least one category then the protocol data unit is released. If they share no categories then the protocol data unit is dropped and the instructions specified in Section 5.6.6 for "incoming violation" are followed.

c. After the proper forwarding output channel is selected the protocol data unit's ORC list will be checked against the RELEASE-CATEGORIES-PORT-OUT list. If the two lists share at least one category then the protocol data unit is released. If they share no categories then the protocol data unit is dropped and the instructions specified in Section 5.6.6 for "forwarding violation" are followed.

5.8.4 Destination System

Follow procedures a and b described in Section 5.8.3 above.

5.8.5 Processing Tag Type 6

In order for a CSL data unit to be forwarded it must pass the following test if it contains a type 6 tag. The CSL processor will contain a binary valued vector $V^R = (v_0, v_1, \dots, v_n)$ where the $v_i = 0$ or 1 , associated with the DOI in the CSL. Call the release map in the CSL tag $V^C = (v_0, v_1, \dots, v_m)$, then if one or more 0s in V^C are in the same position as 0s in V^R the test is passed. Notice the m in V^C can be less than the n in V^R since trailing octets with all 1s are not transmitted in CSL release tags. In performing tests the V^R can be truncated to the length of V^C or the CSL tag can be extended by adding 1s. Given that $m = n$ then if the vector sum $V^R + V^C$ contains one or more 0s the test is passed.

6.0 Key Words

CIPSO
Common Security Label
CSL
DCPS
DTMP
DTMP WG-3
Label Standard
Mandatory Access Control(MAC)
Sensitivity Security Class Tags
Registration
Release Markings Security Policy (RMSP)Security Label
Protocol data unit
Security Label Specification
Sensitivity hierarchical level
SSL